Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method, comprising:

dynamically generating a first set of integrity information for a first processing system during boot operations for said first processing system by selecting an application needed by said first processing system during said boot operations from a plurality of applications to be executed by said first processing system and generating said first set of integrity information for said application using a cryptographic algorithm, the first processing system comprising a first processor of a device;

sending said first set of integrity information to a second processing system that has completed trusted boot operations to verify integrity of said application prior to execution of said application by said first processing system, the second processing system comprising a second processor of the device; ~~and~~

generating an attestation value for said first processing system by said second processing system using said first set of integrity information and a dynamic attestation module connected to said second processing system prior to execution of said application by said first processing system; and

communicating control signals, by the second processing system, to disable access by the first processing system to a transceiver of the device if the integrity of the application is not verified.

2. (Canceled)

3. (Original) The method of claim 1, wherein generating said attestation value comprises:

retrieving a second set of integrity information for said first processing system;

comparing said first set of integrity information with said second set of integrity information; and

generating said attestation value in accordance with said comparison.

4. (Original) The method of claim 1, wherein said sending comprises:

encrypting said integrity information using a first key for said first processing system; and

sending said encrypted integrity information to said second processing system.

5. (Original) The method of claim 4, further comprising authenticating said integrity information prior to generating said attestation value.

6. (Original) The method of claim 5, wherein said authenticating comprises:

receiving said encrypted integrity information;

retrieving a second key for said first processing system; and

decrypting said encrypted integrity information using said second key.

7. (Currently Amended) A method, comprising:

dynamically generating, at a first processor of a device, a first set of integrity information for a first process during boot operations by selecting an application needed by said first process during said boot operations from a plurality of applications to be executed by said first process and generating said first set of integrity information for said application using a cryptographic algorithm;

sending said first set of integrity information to a second processor of the device to perform a second process after the second processor ~~that~~ has completed trusted boot operations to verify integrity of said application prior to execution of said application by said first process; ~~and~~

generating an attestation value for said first process by said second process using said first set of integrity information and a dynamic attestation module prior to execution of said application by said first process; and

communicating control signals, by the second process, to disable access by the first process to a transceiver of the device if the integrity of the application is not verified.

8. (Original) The method of claim 7, wherein said first process and said second process are executed by different processing systems.

9. (Currently Amended) A system, comprising:

an antenna;

a transceiver to connect to said antenna;

a first processing system to connect to said transceiver, said first processing comprising a plurality of applications and a first processor;

a second processing system to connect to said transceiver and said first processing system, said second processing system comprising a second processor; and

a dynamic attestation module to connect to said first and second processing systems, said second processing system to perform dynamic attestation for one of said applications to be executed by said first processing system using said dynamic attestation module after said second processing system has complete trusted boot operations, wherein said dynamic attestation module comprises an integrity module to dynamically generate a first set of integrity information for an application during said boot operations for said first processing system by selecting an application needed by said first processing system during said boot operations from a plurality of applications to be executed by said first processing system and generating said first set of integrity information for said application using a cryptographic algorithm prior to execution of said application by said first processing system, and communicate control signals, by the second processing system, to disable access by the first processing system to the transceiver if the integrity of the application is not verified.

10. (Canceled)

11. (Previously Presented) The system of claim 9, wherein said dynamic attestation module retrieves a second set of integrity information for said application.

12. (Original) The system of claim 11, wherein said dynamic attestation module comprises an attestation module to generate an attestation value for said application by comparing said first set of integrity information with said second set of integrity information.

13. (Previously Presented) The system of claim 9, wherein said dynamic attestation module comprises an authentication module to authenticate said first set of integrity information.

14. (Original) The system of claim 12, wherein said second processing system communicates control signals to said transceiver, said second processing system to disable access to said transceiver by said first processing system in accordance with said attestation value.

15. (Currently Amended) An apparatus, comprising:

a first processing system comprising a plurality of applications and a first processor;

a second processing system to connect to said first processing system, the second processing system having a second processor; and

a dynamic attestation module to connect to said first and second processing systems, said dynamic attestation module to perform dynamic attestation for one of said applications after said second processing system has complete trusted boot operations, wherein said dynamic attestation module comprises an integrity module to dynamically generate a first set of integrity information for said application during said boot operations for said first processing system by selecting an application needed by said first

processing system during said boot operations from a plurality of applications to be executed by said first processing system, and generating said first set of integrity information for said application using a cryptographic algorithm prior to execution of said application by said first processing system, and communicate control signals, by the second processing system, to disable access by the first processing system to a transceiver of the apparatus if the integrity of the application is not verified.

16. (Canceled)

17. (Previously Presented) The apparatus of claim 15, wherein said dynamic attestation module retrieves a second set of integrity information for said application.

18. (Original) The apparatus of claim 17, wherein said dynamic attestation module comprises an attestation module to generate an attestation value for said application by comparing said first set of integrity information with said second set of integrity information.

19. (Previously Presented) The apparatus of claim 15, wherein said dynamic attestation module comprises an authentication module to authenticate said first set of integrity information.

20. (Currently Amended) An article comprising:

a computer-readable storage medium;

said computer-readable storage medium including stored instructions that, when executed by a processor, are operable to dynamically generate a first set of integrity information for a first processing system during boot operations for said first processing system using stored instructions operable to select an application needed by said first processing system during said boot operations from a plurality of applications to be executed by said first processing system, and generate said first set of integrity information for said application using a cryptographic algorithm, the first processing

system comprising a first processor of a device, send said first set of integrity information to a second processing system that has completed trusted boot operations to verify integrity of said application prior to execution of said application by said first processing system, the second processing system comprising a second processor of the device, ~~and~~ generate an attestation value for said first processing system by said second processing system using said first set of integrity information prior to execution of said application by said first processing system, and communicate control signals, by the second processing system, to disable access by the first processing system to a transceiver of the device if the integrity of the application is not verified.

21. (Canceled).

22. (Original) The article of claim 20, wherein the stored instructions, when executed by a processor, generate said attestation value using stored instructions operable to retrieve a second set of integrity information for said first processing system, compare said first set of integrity information with said second set of integrity information, and generate said attestation value in accordance with said comparison.